

Security Architecture

Title	Education, Training and Awareness Policy
Category	Security Architecture
Date Adopted	January 23, 2001
Date of Last Revision	October 31, 2000

A. Authority

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

B. Purpose and Objectives

The purpose of this document is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of the state's information technology resources.

A policy on Education, Training and Awareness is intended to support information security by communicating security needs, best practices, and procedures to all stakeholders. Adequate training of information technology staff is essential to effective implementation of security.

The primary objectives of the Education, Training and Awareness Policy are:

1. To communicate responsibilities for the Education, Training and Awareness of information security policies and procedures;
2. To provide adequate skills for technical staff responsible for implementing security procedures;
3. To establish specific requirements for achieving the goals of Education, Training, and Awareness.
4. To communicate the consequences of violations of security procedures.

Section D provides key definitions.

Section E explains applicability.

Section F describes roles and responsibilities.

C. Education, Training and Awareness Policy**POLICY STATEMENT**

The information security policies and procedures of the agency or institution will be communicated to all employees. Information security policy and procedures will be available for reference and review by employees, contractors, agents acting on behalf of the state and all others in a position to impact the security and integrity of the information assets of the state. A program to maintain effective awareness of information security policy, standards and acceptable practices will exist. Persons responsible for information technology resources must have adequate training on implementing proper security controls for the equipment, software, and networks under their control.

Security Architecture

EXPLANATION

Established security policy and standards must be followed to achieve the intended level of information security, control and integrity.

Information security policy and standards are ineffective if individuals at any level of the organization are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is “a state of mind” that can best be achieved by a program or process that reinforces the concern and appropriate actions on a regular and ongoing basis.

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow policy or practice standards for any reason reduces the value of such statements to “documents of prosecution” and negates the positive reinforcement and protective intent for which the information policy and standards exist.

Information Security is not a one-time event, nor is it a “volume of rules sitting on the shelf.” Good security practices are not always obvious, intuitive or easily incorporated into established routines. To have maximum effectiveness information security standards must be known, understood, believed to have value, and appropriately and consistently practiced.

Effective information security is most nearly achieved when it is a part of everyone’s thinking with regard to daily operations and assignments. A program that reinforces the organization’s position with regard to handling the many aspects of information security provides the tone and commitment to support greater sensitivity to the potential of an unwanted compromise or loss of assets.

Ongoing and positive reinforcement for the necessity for information security policy and standards provides awareness and a “mind set” that encourages the intended practice of the established procedures. Without such reinforcement, policies or standards may be perceived as not relevant, necessary or valuable and may be “followed” but not be practiced in a manner that supports full effectiveness.

STANDARDS

1. All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees with access to critical systems or sensitive information will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.
2. All users must be informed that any actions taken under their assigned identification (e.g., userid) are their responsibility.
3. A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee with access to critical systems or sensitive information.

Security Architecture

4. Important aspects of information security policy and standards will be communicated on a regular basis through postings, distributions, logon screens, meetings or other means that provide regular and useful reminders concerning information security policy and standards.
5. Contractors, agents acting on behalf of the state, auditors, and other non-employees in a position to impact the security or integrity of information assets of the state will be made aware of the Information Security Policy. These individuals must sign a statement acknowledging they have received and read the policy and understand their responsibilities.
6. Persons responsible for information technology resources must be aware of the information security policies and must be knowledgeable about effective security practices for the technical environment under their control.
7. The agency security officer will develop and disseminate guidelines and examples for users to assist them in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, etc., and should include but not be limited to information on passwords and password protection, logon id, virus protection strategies, etc.

D. Key Definitions

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Critical Systems are those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
3. Disaster refers to any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
4. E-mail is the exchange and or sharing of messages, attachments, and calendar and scheduling information.
5. Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.
6. Security Policy is a statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
7. Security Standard is a set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
8. Sensitive Information is that information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
9. State Data Communications Network (SDCN) shall mean any data communications facility contracted for or provided by the State of Nebraska,

Security Architecture

including State-provided Internet access and network connections to state computers.

10. Users of electronic assets include any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
11. Value of information includes the cost of collection, cost of reconstruction, and legal or operational consequences if information is lost or compromised.

E. ApplicabilityGENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Each agency or operational entity must develop detailed procedures to implement broad policies and standards. Compliance with these security policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC. Compliance may be used in audit reviews or budget reviews.

EXCEPTION STATEMENT

"Computer security must support the mission of the organization." "The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected." "Owners of sensitive information and critical systems have security responsibilities outside their organization." (From the Information Security Management Policy)

These three principles provide the basis for determining the applicability of security policies and standards to specific situations within an organization. The responsible security authority of an organization should establish a two-step test, before exempting a unit within the organization from a particular security requirement. The first test is met, if a security requirement is contrary to the organization's mission or is not cost-effective given the value of the assets being protected. The second test is met, if exempting a security requirement does not create unreasonable risk of adverse consequences to people or entities outside of the organization. Both tests should be met.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information security program. Such policies should be effective and commensurate with the risks involved. The NITC intends to incorporate adherence to security policies as part of its evaluation and prioritization of funding requests. The NITC recommends that the Governor and Legislature give due consideration to requests for security improvements during the budget process.

F. Responsibility

An effective security program involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of

Security Architecture

information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate security of information systems through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of information security programs.

2. Technical Panel Security Work Group. The NITC Technical Panel, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.
3. Chief Information Officer, State of Nebraska. The CIO has the responsibility to assist in building the business case for cost-effective implementation of security programs in non-education state agencies. The CIO must also work with non-education state agencies to coordinate and evaluate security programs. The CIO shall insure that non-education state agencies have documented procedures to demonstrate compliance with these security policies.
4. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
5. Agency Information Officer. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies.
6. Agency Security Officer. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for:
 - Implementing enterprise and agency-specific or application-specific security policies and procedures.
 - Developing procedures and administering the information access control decisions made by information custodians within the agency.
 - Identifying training requirements.
 - Implementing procedures for authentication of users and messages.
 - Publish guidelines for creating and managing passwords.
 - Developing and implementing strategies to make users aware of security policies, procedures and benefits.
 - Documenting the security support structure across platforms.
 - Enforcing agency security policies.
 - Establishing and chairing agency security committees.
 - Monitoring unusual activities and report security breaches and incidents.
 - Periodically evaluating effectiveness of security policies and procedures.

Security Architecture

- Fact gathering and analysis on information security issues.
- Developing recommendations for the agency or institution on security matters.
- Reviewing changes to the configuration of security administration facilities and settings.
- Participate in preparing a disaster recovery plan. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan.

The Agency Security Officer may work with a security committee of the agency or institution. The Security Committee is an advisory group made up of key technical and management personnel within the agency to coordinate security efforts and resolve security problems.

7. Program Managers and Information Custodians. In most cases, the authority within the agency or institution delegates custody of specific types of information maintained by the agency to administrators in the agency who may further delegate to employees in their organizations. These persons have direct responsibility for:
 - deciding issues pertaining to access to information
 - insuring information security
 - participating in preparing a disaster recovery plan.
8. Users of Electronic Assets. All authorized users shall be accountable for their actions relating to information assets, including hardware, software and electronic information. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.
9. Information Technology Staff. Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. People with access management rights must follow strict procedures regarding their access to information resources and sharing that access with others.
10. Employees and persons under contract. Employees must become knowledgeable about their organization's security policies and procedures. Employees must exercise due diligence in following those procedures and incorporating sound security practices in the discharge of their normal duties.

G. Related Policies, Standards and Guidelines

The Information Security Management Policy provides the general requirements for a set of policies, standards, and procedures to protect the information assets of an organization. Other information security policies address the specific topics of:

1. Access Control Policy
2. Disaster Recovery Policy
3. Education, Training and Awareness Policy
4. Individual Use Policy
 - Acceptable Use
 - Copyrighted Materials
 - E-mail Use

Security Architecture

5. Network Security Policy
 - General Network Controls
 - Perimeter Security for Internet and Intranet Connections
 - Remote Access
6. Security Breaches / Incident Reporting Policy